THE GROUP STRUCTURE OF BACHET ELLIPTIC CURVES OVER FINITE FIELDS $\mathbb{F}_p$

Nazlı Yıldız İkikardeş, Musa Demirci, Gökhan Soydan,

İsmail Naci Cangül

Abstract

Bachet elliptic curves are the curves $y^2 = x^3 + a^3$ and in this work the group structure $E(\mathbb{F}_p)$ of these curves over finite fields $\mathbb{F}_p$ is considered. It is shown that there are two possible structures $E(\mathbb{F}_p) \cong C_{p+1}$ or $E(\mathbb{F}_p) \cong C_n \times C_{nm}$, for $m, n \in \mathbb{N}$, according to $p \equiv 5 \pmod 6$ and $p \equiv 1 \pmod 6$, respectively. A result of Washington is restated in a more specific way saying that if $E(\mathbb{F}_p) \cong Z_n \times Z_n$, then $p \equiv 7 \pmod{12}$ and $p = n^2 \mp n + 1$.

1 Introduction

[1][2]Let p be a prime. We shall consider the elliptic curves

$$E: \ y^2 \equiv x^3 + a^3 \pmod p \tag{1}$$

where a is an element of $\mathbb{F}_p^* = \mathbb{F}_p - \{0\}$. Let us denote the group of the points on E by $E(\mathbb{F}_p)$.

If $\mathbb{F}$ is a field, then an elliptic curve over $\mathbb{F}$ has, after a change of variables, a form

$$y^2 = x^3 + Ax + B$$

where A and $B \in \mathbb{F}$ with $4A^3 + 27B^2 \neq 0$ in $\mathbb{F}$. Here $D = -16\left(4A^3 + 27B^2\right)$ is called the discriminant of the curve. Elliptic curves are studied over finite and infinite fields. Here we take $\mathbb{F}$ to be a finite prime field $\mathbb{F}_p$ with characteristic $p > 3$. Then $A, B \in \mathbb{F}_p$ and the set of points $(x, y) \in \mathbb{F}_p \times \mathbb{F}_p$, together with a *point o at infinity* is called the set of $\mathbb{F}_p-$ *rational points* of E on $\mathbb{F}_p$ and is denoted by $E(\mathbb{F}_p)$. N_p denotes the number of rational points on this curve. It must be finite.

In fact one expects to have at most $2p+1$ points (together with o)(for every x, there exist a maximum of 2 $y^{'}$s). But not all elements of $\mathbb{F}_p$ have square

---

roots. In fact only half of the elements of $\mathbb{F}_p$ have a square root. Therefore the expected number is about $p + 1$.

It is known that

$$N_p = p + 1 + \sum_{x=0}^{p-1} \chi\left(x^3 + Ax + B\right).$$

Here we use the fact that the number of solutions of $y^2 \equiv u \quad (p)$ is $1 + \chi\left(u\right)$.

The following theorem of Hasse quantifies this result.

Theorem 1 (Hasse 1922) $N_p < \left(\sqrt{p} + 1\right)^2$.

Now we look at the algebraic structure of $E\left(\mathbb{F}_p\right)$.

Let $P\left(x_1, y_1\right)$ and $Q\left(x_2, y_2\right)$ be two points on $E : y^2 = x^3 + Ax + B$.

Let also

$$m = \begin{cases} \left(y_2 - y_1\right)/\left(x_2 - x_1\right) & if \quad P \neq Q \\ \left(3x_1^2 + A\right)/2y_1 & if \quad P = Q \end{cases}$$

where $y_1 \neq 0$, while when $y_1 = 0$, the point is of order 2.

$$x_3 = m^2 - x_1 - x_2 \text{ and } y_3 = m\left(x_1 - x_3\right) - y_1$$

then

$$P + Q = \begin{cases} o & if \quad x_1 = x_2 \quad and \ y_1 + y_2 = 0 \\ Q & if \quad P = Q \\ \left(x_3, y_3\right) & \text{otherwise} \end{cases}.$$

By definition $-P = \left(x, -y\right)$.

Because of the definition of addition in an arbitrary field, it takes very long to make any addition and the results are very complicated.

Here we shall deal with Bachet elliptic curves $y^2 = x^3 + a^3$ modulo p. Let $N_{p,a}$ denote the number of rational points on this curve. Some results on these curves have been given in [1], and [2].

A historical problem leading to Bachet elliptic curves is that how one can write an integer as a difference of a square and a cube. In another words, for a given fixed integer c, search for the solutions of the Diophantine equation $y^2 - x^3 = c$. This equation is widely called as Bachet or Mordell equation. The existence of duplication formula makes this curve interesting. This formula was found in 1621 by Bachet. When (x, y) is a solution to this equation where $x, \ y \in \mathbb{Q}$, it is easy to show that $\left(\frac{x^4 - 8cx}{4y^2}, \frac{-x^6 - 20cx^3 + 8c^2}{8y^3}\right)$ is also a solution for the same equation. Furthermore, if (x, y) is a solution such that $xy \neq 0$ and $c \neq 1, \ -432$, then this leads to infinitely many solutions, which could not proven by Bachet. Hence if an integer can be stated as the difference of a cube and a square, this could be done in infinitely many ways.

If $p \equiv 5 \pmod 6$, it is well known that $E(\mathbb{F}_p) \cong C_{p+1}$, the cyclic group of order $p+1$, [4]. But when $p \equiv 1 \pmod 6$, there is no result giving the group structure of $E(\mathbb{F}_p)$. In this work, we discuss this situation. We show that this group is isomorphic to a direct product of two cyclic groups C_n and C_{nm}, i.e.

$$E(F_p) \cong C_n \times C_{nm}$$

for $m, n \in \mathbb{N}$. If we denote the order of $E(\mathbb{F}_p)$ by $N_{p,a}$, then

$$N_{p,a} = n^2 m = p + 1 - b$$

where $b > 0$ when $a \in Q_p$, and $b < 0$ otherwise. Here b is the trace of the Frobenius endomorphism.

2 Bachet Elliptic curves having a group of the form $C_n \times C_{nm}$

Let E be the curve in (1). Then its twist is defined as the curve $y^2 \equiv x^3 + g^3 a^3$, where g is an element of Q'_p, the set of quadratic non-residues modulo p. As usual, Q_p denotes the set of quadratic residues modulo p. Here note that if $a \in Q_p$, then $ga \in Q'_p$ and when $a \in Q'_p$, then $ga \in Q_p$. It is easy to show that b of (1) and of its twist have different signs. Therefore

Theorem 2 *Let $p \equiv 1 \pmod 6$ be a prime. If (1) has the group isomorphic to $C_n \times C_{nm}$ with order $n^2 m = p + 1 - b$, then its twist is isomorphic to $C_r \times C_{rs}$ with order $r^2 s = p + 1 + b$.*

Let us define $t = |b|$. That is

$$t = |p + 1 - N_{p,a}|.$$

We first have

Theorem 3 *a) Let $p \equiv 1 \pmod{12}$ be a prime. Then*

$$b \equiv 2 \pmod{12} \ iff \ N_{p,a} \equiv 0 \pmod{12}$$

and

$$b \equiv 10 \pmod{12} \ iff \ N_{p,a} \equiv 4 \pmod{12}.$$

b) Let $p \equiv 7 \pmod{12}$ be a prime. Then

$$b \equiv 4 \pmod{12} \ iff \ N_{p,a} \equiv 4 \pmod{12}$$

and

$$b \equiv 8 \pmod{12} \ iff \ N_{p,a} \equiv 0 \pmod{12}.$$

Proof. a) Let $p \equiv 1 \pmod{12}$ be a prime. Then we can write this as $p = 1 + 12n$, $n \in \mathbb{Z}$. Also $b \equiv 2 \pmod{12}$ can be stated as $b = 2 + 12m$, $m \in \mathbb{Z}$. By substituting these, we get

$$b \equiv 2 \pmod{12} \iff N_{p,a} = p + 1 - b$$

and hence $N_{p,a} = 1 + 12n + 1 - (2 + 12m) = 12(n - m)$ and this is only valid when $N_{p,a} \equiv 0 \pmod{12}$. Similarly,

$$b \equiv 10 \pmod{12} \iff N_{p,a} = p + 1 - b = 1 + 12n + 1 - (10 + 12m)$$

and therefore $N_{p,a} = -8 + 12(n - m)$ and this means that $N_{p,a} \equiv 4 \pmod{12}$. Part b) is proved in a similar fashion. ∎

Theorem 4 *Let $p \equiv 1 \pmod{6}$ be a prime. Then b is not divisible by 6.*

Proof. Let us consider the curve $y^2 = x^3 + 1$. It has a point of order 6. Therefore its reduction modulo p has also a point of order 6. Therefore

$$b \equiv p + 1 - N_{p,a} \equiv 2 - 0 \equiv 2 \pmod{6}.$$

The other possibility for the curve is $y^2 = x^3 + a^3$ with a is a quadratic non-residue. It is the quadratic twist of the other curve, so has $b \equiv -2 \pmod{6}$. Therefore in both cases b is non-zero mod 6. ∎

Corollary 5 *Let $p \equiv 1 \pmod{6}$ be a prime. Then $N_{p,a} \equiv 0$ or $N_{p,a} \equiv 4 \pmod{6}$.*

Also one obtains the following result:

Corollary 6 *If $p \equiv 1 \pmod{12}$ is a prime, then $b \equiv \mp 2 \pmod{12}$ and if $p \equiv 7 \pmod{12}$ is a prime, then $b \equiv \mp 4 \pmod{12}$.*

We now have the following result about the number of points on curves (1).

Theorem 7 *Let $p \equiv 1 \pmod{6}$ be a prime. Then*
a) If $t \equiv 2 \pmod{6}$, then (1) has $b = t$ and $N_{p,a} \equiv 0 \ (6)$, and its twist has $b = -t$ and $N_{p,a} \equiv 4 \pmod{6}$.
b) If $t \equiv 4 \pmod{6}$, then (1) has $b = t$ and $N_{p,a} \equiv 4 \pmod{6}$, and its twist has $b = -t$ and $N_{p,a} \equiv 0 \pmod{6}$.

Proof. Let $p \equiv 1 \pmod{6}$ be a prime. Let us put $p = 1 + 6n$, $n \in \mathbb{Z}$. Let $t = 2 \pmod{6}$. If $b = t$, then $b \equiv 2 \pmod{6}$ and now put $b = 2 + 6m$, $m \in \mathbb{Z}$. Therefore

$$\begin{aligned} N_{p,a} &= p + 1 - b = 6n + 1 + 1 - 2 - 6m \\ &= 6(n - m) \end{aligned}$$

implying $N_{p,a} \equiv 0 \pmod{6}$.

The other parts can be proven similarly. ∎

We then immediately have the following result concerning the elements of order 3:

Corollary 8 *a) Let $p \equiv 1 \pmod{12}$ be a prime. If $t \equiv 2 \pmod{12}$, then (1) has $b = t$ and $N_{p,a} \equiv 0 \pmod{12}$ and $E(\mathbb{F}_p)$ has elements of order 3. Its twist has $b = -t$ and $N_{p,a} \equiv 4 \pmod{12}$ implying that there are no elements of order 3.*

If $t \equiv 10 \pmod{12}$, then (1) has $b = t$ and $N_{p,a} \equiv 4 \pmod{12}$ and $E(\mathbb{F}_p)$ has no elements of order 3, while its twist has $b = -t$ and $N_{p,a} \equiv 0 \pmod{12}$ implying that the group has elements of order 3.

b) Let $p \equiv 7 \pmod{12}$ be a prime. If $t \equiv 4 \pmod{12}$, then (1) has $b = t$ and $N_{p,a} \equiv 4 \pmod{12}$ and therefore has no points of order 3, while its twist has $b = -t$ and $N_{p,a} \equiv 0 \pmod{12}$ having elements of order 3.

If $t \equiv 8 \pmod{12}$, then (1) has $b = t$ and $N_{p,a} \equiv 0 \pmod{12}$ implying it has elements of order 3 while its twist has $b = -t$ and $N_{p,a} \equiv 4 \pmod{12}$ having no such elements.

The elements of order 3 are important in the classification of these elliptic curves modulo p. We now show that their number is either 2 or 8:

Theorem 9 *Let $p \equiv 1 \pmod{6}$ be a prime. If $N_{p,a} \equiv 0 \pmod{6}$, then there are 2 or 8 points of order 3.*

Proof. By [5], there are at most 9 points together with the point at infinity o, forming a subgroup which is either trivial, cyclic of order 3 or the direct product of two cyclic groups of order 3. As we want to determine the number of elements of order 3, this group cannot be trivial. Then it is C_3 or $C_3 \times C_3$ and it is well-known that it contains 2 or 8 elements of order 3, respectively. ■

In fact, if we let $E(\mathbb{F}_p) \cong C_n \times C_{nm}$, then when 3 divides n, $E(\mathbb{F}_p)$ has 8 points of order 3, and when not, it has 2 points of order 3.

We are now going to give one of the main results in Theorem 13. We first need the following results:

Corollary 10 *Let p be a prime. Then for only $x = 0$ among all values of x in $\mathbb{F}_p$, $x^3 + 1$ takes the value 1.*

Proof. It is clear that $x = 0$ satisfies the condition. The fact that no other value of x satisfies $x^3 + 1 = 1$ is clear from the fact p is prime. ■

Theorem 11 *Let $p \equiv 1 \pmod{6}$ be a prime. There are 3 values of x between 1 and p so that $x^3 + 1 \equiv 0 \pmod{p}$.*

Proof. It is obvious that $x^3 \equiv a \pmod{p}$ has three solutions in $\mathbb{F}_p$ for every $a \neq 0$. For $a = -1$, the proof follows. ■

Theorem 12 *Let $p \equiv 1 \pmod{6}$ be a prime. Then*

$$\sum_{x \in \mathbb{F}_p} \chi\left(x^3 + 1\right) \equiv 4 \pmod{6}.$$

Proof. For each $x \in \mathbb{F}_p$, calculate the p values of $x^3 + 1$. By Theorem 10, one of these values is 1. By Theorem 11, three of them are 0. The rest $p - 4$ values of $x^3 + 1$ are grouped into $\frac{p-4}{3}$ triples. As $p \equiv 1 \pmod 6$, $\frac{p-4}{3}$ is odd. Indeed, let us write $p = 1 + 6k$, $k \in \mathbb{Z}$. Then $\frac{p-4}{3} = 2k - 1$. Let us suppose that out of these triples, s triples are in Q_p and $2k - 1 - s$ are in Q'_p. If a triple is in Q_p, then it adds $+3$ to the sum $\sum_{x \in \mathbb{F}_p} \chi\left(x^3 + 1\right)$, and if it is in Q'_p, -3 is added. Therefore

$$\sum_{x \in \mathbb{F}_p} \chi\left(x^3 + 1\right) = 1 + 3.0 + s.(+3) + (2k - 1 - s).(-3)$$

$$= 6(s - k) + 4$$

implying the result. ∎

Theorem 13 *Let $p \equiv 1 \pmod 6$ be a prime. $a \in Q_p$ iff $N_{p,a} \equiv 0 \pmod 6$.*

Proof. It is well-known that

$$N_{p,a} = p + 1 + \sum_{x \in \mathbb{F}_p} \chi\left(x^3 + a^3\right)$$

By putting $p = 1 + 6n$ for $n \in \mathbb{Z}$, we get $N_{p,a} = 6n + 2 + \sum_{x \in \mathbb{F}_p} \chi\left(x^3 + a^3\right)$. Now as $\chi(a) = 1$, and as the set of the values of x^3 is the same as the set of the values of $a^3 x^3$, we can write

$$\sum_{x \in \mathbb{F}_p} \chi\left(x^3 + a^3\right) = \sum_{x \in \mathbb{F}_p} \chi\left(a^3 x^3 + a^3\right)$$

$$= \sum_{x \in \mathbb{F}_p} \chi\left(a^3\right) \chi\left(x^3 + 1\right)$$

$$= \sum_{x \in \mathbb{F}_p} \chi\left(x^3 + 1\right),$$

and by Theorem 12, this sum is congruent to 4 modulo 6. Hence, by putting $\sum_{x \in \mathbb{F}_p} \chi\left(x^3 + a^3\right) = 4 + 6r$, $r \in \mathbb{Z}$, we get $N_{p,a} = 6n + 2 + 4 + 6r$ implying $N_{p,a} \equiv 0 \pmod 6$. ∎

Corollary 14 *Let $p \equiv 1 \pmod 6$ be a prime. If $N_{p,a} \equiv 0 \pmod 6$, then $b \equiv 2 \pmod 6$.*

Proof. As $N_{p,a} = p + 1 - b = p + 1 + \sum_{x \in \mathbb{F}_p} \chi\left(x^3 + a^3\right)$, we know that $b = -\sum_{x \in \mathbb{F}_p} \chi\left(x^3 + a^3\right)$. By Theorem 12, the result follows. ∎

Similarly we have

Theorem 15 *Let $p \equiv 1 \pmod 6$ be a prime. Then $a \in Q'_p$ iff $N \equiv 4 \pmod 6$.*

Corollary 16 *Let $p \equiv 1 \pmod 6$ be a prime. Let E be the curve given by (1). Then*

    a) $a \in Q_p$ iff $E(\mathbb{F}_p)$ has 2 or 8 elements of order 3.
    b) $a \in Q_p^{'}$ iff $E(\mathbb{F}_p)$ has no elements of order 3.

Proof. It is clear from Corollary 8 and Theorem 13. ∎

3 Bachet Elliptic Curves having a group of the form $C_n \times C_n$.

Now we shall consider the case where the Bachet elliptic curves have a group isomorphic to $C_n \times C_n$ for same n. This is only possible when $p \equiv 1 \pmod 6$, as otherwise when $p \equiv 5 \pmod 6$, $E(\mathbb{F}_p)$ is isomorphic to the cyclic group C_{p+1}. We shall consider a result of Washington and refine it:

Theorem 17 *[3] Let E be an elliptic curve over $\mathbb{F}_q$ where q is a prime power and suppose $E(\mathbb{F}_q) \cong \mathbb{Z}_n \times \mathbb{Z}_n$ for some integer n. Then either $q = n^2 + 1$, $q = n^2 \mp n + 1$ or $q = (n \mp 1)^2$.*

Now we give a more specific result for Bachet elliptic curves given by (1) over $\mathbb{F}_q$:

Theorem 18 *Let E be the elliptic curve in (1). Suppose*

$$E(\mathbb{F}_p) \cong \mathbb{Z}_n \times \mathbb{Z}_n.$$

Then $p \equiv 7 \pmod{12}$ and $p = n^2 \mp n + 1$.

Proof. By Theorem 17, there are three possibilities $p = n^2+1$, $p = n^2 \mp n+1$ or $p = n^2 \mp 2n+1$. The latter one is immediately rules out as p cannot be a square. We need only show that p cannot be equal to $n^2 + 1$.

If $p = n^2 + 1$, than $n^2 = p - 1$ and hence $p - 1$ is in Q_p. But it is known that $p - 1$ could be in Q_p only when $p \equiv 1, 5 \pmod{12}$ is prime. Therefore the result follows. ∎

References

[1] Demirci, M. & Soydan, G. & Cangül, I. N., *Rational points on the elliptic curves $y^2 = x^3 + a^3 \pmod p$ in $\mathbb{F}_p$ where $p \equiv 1 \pmod 6$ is prime,* Rocky Mountain Journal Of Mathematics,Vol.37, No:5 (2007), 1467-1475.

[2] Soydan, G. & Demirci, M. & Ikikardeş, N. Y. & Cangül, I. N., *Rational points on the elliptic curves $y^2 = x^3 + a^3 \pmod p$ in $\mathbb{F}_p$ where $p \equiv 5 \pmod 6$ is prime,* International Journal Of Mathematics Sciences, Vol.1, No:4 (2007), 247-250.

[3] Washington, L. C., *Elliptic Curves, Number Theory and Cryptography,* Chapman&Hall/CRC, 2003

[4] Schmitt, S., Zimmer, H. G., *Elliptic Curves,a computational approach,* Walter de Gruyter, 2003

[5] Schoof, R., *Nonsingular Plane Cubic Curves over Finite Fields,* J.Comb. Thry., Ser. A, Vol. 46, No: 2, 1987

Musa Demirci, Gökhan Soydan, İsmail Naci Cangül
Department of Mathematics
Uludağ University
16059 Bursa, TURKEY
mdemirci@uludag.edu.tr, gsoydan@uludag.edu.tr, cangul@uludag.edu.tr
Nazlı Yıldız İkikardeş
Department of Mathematics
Balıkesir University
Balıkesir, TURKEY
nyildiz@balikesir.edu.tr